



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,882	04/04/2001	Mark Buer	BRCMP006/BP	5560

7590 11/10/2004

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER

NORRIS, TREMAYNE M

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/827,882

Applicant(s)

BUER ET AL.

Examiner

Tremayne M. Norris

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 April 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 9-12, 14, 16-22, 24, 25, 27, 29 and 30 is/are rejected.
- 7) ☒ Claim(s) 7, 8, 13, 15, 23, 26, 28 and 31 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/29/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3,16-22,27 are rejected under 35 U.S.C. 102(e) as being anticipated by Silverbrook et al (US pat 6,334,190).

Regarding claim 1, Silverbrook teaches an authentication engine architecture for an multi-loop, multi-round authentication algorithm, comprising:

a first instantiation of a multi-round authentication algorithm hash round logic in an inner hash engine (col.7 lines 3-5; col.11 lines 9-27);

a second instantiation of a multi-round authentication algorithm hash round logic in an outer hash engine (col.7 lines 3-5; col.11 lines 9-27);

a dual-frame payload data input buffer configured for loading one new data block while another data block one is being processed in the inner hash engine (col.7 lines 3-5; col.45 lines 2-6);

an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations (col.45 lines 2-6); and

a dual-port ROM configured for concurrent constant lookups for both inner and outer hash engines (col.38 lines 8-13).

Regarding claim 2, Silverbrook teaches the multi-loop, multi-round authentication algorithm is HMAC-MD5 (col.11 lines 4-9).

Regarding claim 3, Silverbrook teaches the multi-loop, multi-round authentication algorithm is HMAC-SHA1 (col.11 lines 4-9).

Regarding claim 16, Silverbrook teaches a method of authenticating data transmitted over a computer network, comprising:

receiving a data packet stream;
splitting the packet data stream into fixed-size data blocks (col.7 lines 3-5); and
processing the fixed-size data blocks using a multi-loop, multi-round authentication engine architecture having a hash engine core comprising an inner hash engine and an outer hash engine, said architecture configured to,
pipeline hash operations of said inner hash and outer hash engines,
collapse and rearrange multi-round logic to reduce rounds of hash operations,
and

implement multi-round logic to schedule addition computations to be conducted in parallel with round operations (col.11 lines 9-27).

Regarding claim 17, Silverbrook teaches said pipelining comprises performance of an outer hash operation for one data payload in parallel with an inner hash operation of a second data payload in a packet stream fed to the authentication engine (col.11 lines 9-27).

Regarding claim 18, Silverbrook teaches a dual frame input buffer is used for the inner hash (col.11 lines 9-27; col.45 lines 2-6).

Regarding claim 19, Silverbrook teaches the initial hash states for the hash operations are double buffered for concurrent inner hash and outer hash operations (col.11 lines 9-27; col.45 lines 2-6).

Regarding claim 20, Silverbrook teaches constant lookups are performed from a dual-ported ROM by both inner and outer hash engines (col.11 lines 9-27; col.38 lines 8-13; col.45 lines 2-6).

Method claims 21 and 22 are substantially equivalent to authentication engine claims 2 and 3 respectively, therefore claims 21 and 22 are rejected for the same reasons.

Regarding claim 27, Silverbrook teaches a method of authenticating data transmitted over a computer network, comprising:

receiving a data packet stream;
splitting the packet data stream into fixed-size data blocks (col.7 lines 3-5); and
processing the fixed-size data blocks using a multi-round authentication engine architecture, said architecture implementing hash round logic for a multi-round authentication algorithm configured to schedule addition computations to be conducted in parallel with round operations (col.11 lines 9-27).

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 14, 29, 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier.

Regarding claim 14, Schneier teaches an authentication engine architecture for an SHA1 authentication algorithm, comprising:

at least one hash engine configured to implement hash round logic comprising:

Art Unit: 2137

five hash state registers;

one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative (pages 442-45).

Method claim 29 is substantially equivalent to architecture engine claim 14, therefore claim 29 is rejected for the same reasons.

Regarding claim 30, Schneier teaches registers having the critical path are alternative (pages 442-45).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook, and further in view of Sait et al.

Regarding claim 4, Silverbrook teaches the authentication engine architecture of claim 1 but does not teach a plurality of carry save adders for computation of partial products, and a carry look-ahead adder for computation and propagation of a final sum. Sait teaches a plurality of carry save adders for computation of partial products, and a carry look-ahead adder for computation and propagation of a final sum (figs.3 and 6, page 110 col.2 paragraphs 2 and 3). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Silverbrook's system for the manipulation of secure data with Sait's technique for fast multiplication in order to process large amounts of data at high speeds (Sait page 109 Introduction).

Regarding claim 5, Silverbrook and Sait in combination teach the authentication engine architecture of claim 4, in addition Sait teaches the carry save adders and the carry look-ahead adder are configured such that addition computations are conducted in parallel with round operations (figs.3 and 6, page 110 col.2 paragraphs 2 and 3).

7. Claims 6 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook, and further in view of Schneier.

Art Unit: 2137

Regarding claim 6, Silverbrook teaches the authentication architecture of claim 3. What Schneier teaches that Silverbrook does not teach is

five hash state registers;

one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative (pages 442-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Silverbrook's system for the manipulation of secure data with Schneier's teaching of the secure hash algorithm in order to help ensure the security of a message sent (Schneier page 442).

Method claim 24 is substantially equivalent to authentication engine claim 6, therefore claim 24 is rejected for the same reasons.

8. Claims 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook, and further in view of Sait.

Regarding claim 9, Silverbrook teaches an authentication engine architecture for a multi-round authentication algorithm, comprising:

a hash engine configured to implement hash round logic for a multi-round authentication algorithm, said hash round logic implementation (col.11 lines 9-27).

What Sait teaches that Silverbrook does not teach is at least one addition module comprising teach a plurality of carry save adders for computation of partial products, and a carry look-ahead adder for computation and propagation of a final sum (figs.3 and 6, page 110 col.2 paragraphs 2 and 3). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Silverbrook's system for the manipulation of secure data with Sait's technique for fast multiplication in order to process large amounts of data at high speeds (Sait page 109 Introduction).

Regarding claim 10, Silverbrook and Sait in combination teach the authentication engine architecture of claim 9, in addition Sait teaches the carry save adders and the carry look-ahead adder are configured such that addition computations are conducted in parallel with round operations (figs.3 and 6, page 110 col.2 paragraphs 2 and 3).

Claims 11 and 12 are authentication engine claims that are substantially equivalent to authentication engine claims 2 and 3 respectively, therefore claims 11 and 12 are rejected for the same reasons.

Allowable Subject Matter

9. Claims 7,8,13,15,23,26,28,31 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

With respect to claims 7,15,26,31, the cited prior art fails to specifically teach eighty rounds of an SHA1 loop are collapsed into forty rounds.

With respect to claims 8 and 13, the cited prior art fails to teach:

An authentication engine wherein at least one of the inner and outer hash engines is configured to implement hash round logic comprising:

- five hash state registers;

- a 5-bit circular shifter;

- an add5to1 adder module having a plurality of CSAs and a CLA adder;

- a 30-bit circular shifter; and

- an add4to1 adder module having a plurality of CSAs and a CLA adder.

With respect to claims 23 and 28, the cited prior art fails to specifically teach:

- conducting a 5-bit circular shift on data from a first register;

- adding an initial hash state in a second register, a first payload data block, a first constant, and the result of a function (F_t) of the initial hash states in third, fourth and fifth additional registers with an add5to1 adder module having a plurality of CSAs and a CLA adder;

- conducting a 30-bit circular shift on data from the third additional register; and

- adding the initial hash state in the fourth additional register to a second payload block, a second constant, and the result of a function (F_t) of the initial hash states in the

Art Unit: 2137

first and fifth registers and the shifted hash state of the third register with an add4tol adder module having a plurality of CSAS and a CLA adder.

Conclusion

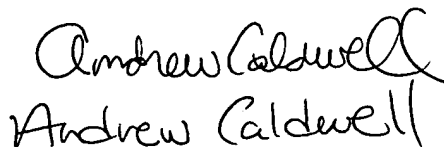
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (571) 272-3874. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

October 24, 2004



Andrew Caldwell